## Question 1:

Answer the following questions by clearly circling *the most appropriate* answer ( 1 point *each*)

1. A loss of _____ is the unauthorized disclosure of information.
   a. integrity
   b. authenticity
   c. reliability
   d. confidentiality

2. What is the inverse of confidentiality, integrity, and availability?
   a. misuse, exposure, destruction
   b. authorization, non-repudiation, integrity
   c. disclosure, alteration, destruction
   d. confidentiality, integrity, availability

3. Implements the security *policies* of the data processing systems and information transfers of an organization
   a. Security attack
   b. Security service
   c. Security encryption
   d. Security mechanism

4. What type of crypto-analytical attack where an adversary has least amount of information to work with?
   a. Known plain text
   b. Cipher text only
   c. Plain text only
   d. Chosen cipher text

5. All encryption algorithms are considered breakable except one which may be considered unbreakable, which is
   a. 3DES with codebooks
   b. RSA with Elliptic-curve
   c. AES with CBC
   d. Onetime pad
   e. iOS SSL Enclave

6. To which stage in AES, if removed, there is no security:
   a. Byte Substitution
   b. Shift Row
   c. Mix Column
   d. Add Round key

7. The practice of embedding a message in a document, image, video or sound recording so that its very existence is hidden is called

   a. anonymity.
   b. steganography.
   c. non-repudiation.
   d. masquerading

8. What is the main step in a AES that is responsible for confusion

   a. The Byte Substitution
   b. The Shift Key
   c. The Mix Column
   d. The Add Round key
   e. All of the above

9. Alice encrypted a message using a cryptographic algorithm three times using three keys of size 16, 32, and 48 bits for encryption. An attacker launched a brute force attack on the keys. On average, how many key attempts expected to know the keys

   a. $2^{93}$
   b. $2^{95}$
   c. $2^{96}$
   d. $2^{47}$
   e. $2^{48}$

10. Monoalphabetics are easy to break because they reflect the frequency data of the original alphabet. A countermeasure is to

    a. provide multiple substitutes.
    b. permute the cipher to be in reverse order.
    c. replace the characters with symbols.
    d. Use Caesar cipher with large key.

## Question 2:

1. Define each of the following: [ 2 points ]

   - unconditional security
     algorethm not
     for a given cipher ~~[illegible]~~ it ~~[illegible]~~ breakable ~~at~~ all even after long time and with all needed of resourses.

   - Authentication
     - encurance that communicatin is withe Authorise user or not.
     ~~or~~ check the user of servecie is Authorised or not.

2. There are 33 letters in the Russian alphabet. 11 vowels, 20 consonants, and 2 pronunciation signs. [ 2 points ]

   a. How large is the key space using monoalphabet?
   33!

   b. Monoalphabetic substitution cipher is not secure. Why?
   because language characteristic, "frequnce in letters".

3. Construct a table for the Playfair Cipher with the keyword "SWAZILAND"? [ 3 points ]
   Then encrypt the phrase: "CRUMBLES"

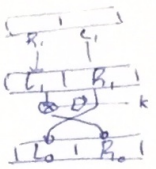
| | | | | |
|---|---|---|---|---|
| S | W | A | Z | I/J |
| L | N | D | B | C |
| E | F | G | H | K |
| M | O | P | Q | R |
| T | U | V | X | Y |

KXOTCNML
TO

4. What is the main weakness of Caesar cipher? [ 1 points ]
   key size only 26, can broken with bruteforce easly.

5. What is the *name* of the two types of operations used for transforming plaintext to ciphertext? [ 1 points ]
   - substetution
   - permentation.

6. Playfair and polyalphabet algorithms both use a keyword. When can polyalphabet (Vigenere) be considered of the same security level as playfair *i.e.* applying same attack? [ 1 points ]
   if we use keyword ~~of size 2 for polyalphabet~~.
   of polyalphabet is fixed for each cuble of letters in the plain text.
   ex. every (ab) in plain text is encripted by (ZO) keyword.



## Question 3:

1. Given the following symbols used in DES { $L_0$, $R_0$, F, XOR, $L_1$, $R_1$, $K_1$ } [ 4 points ]

   i. Write the encryption equations to produce $L_1$ and $R_1$ for one round of DES from $L_0$ and $R_0$

   $L_1 = R_0$

   $R_1 = L_0$ XOR $F(R_0, k)$ ✓

   ii. Write the decryption equations to produce $L_0$ and $R_0$ from $L_1$ and $R_1$ calculated in (a) and prove the equality.

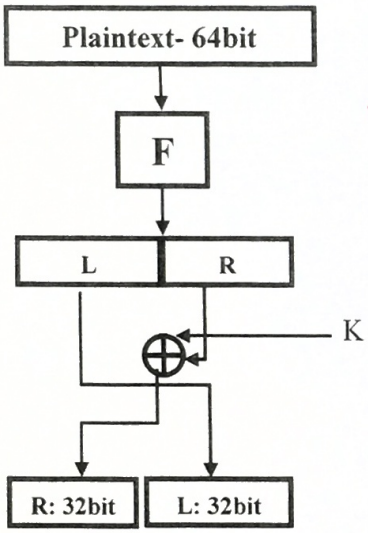
   $L_0 = L_1 = R_0$

   $R_0 = R_1$ XOR $F(L_1, k)$

   $= L_0$ XOR $F(R_0, k)$ XOR $(L_1, k)$ $= L_0$ XOR $0 = L_0$ ✓

   4

2. Below is one round encryption of an algorithm called SES which resembles DES algorithm. [ 5 points ]




   a. List from SES three similar actions to DES

   - swap left with RH ✓
   - XOR key ✓
   - ~~left and RH are 32 bit~~ use F function on plain text. ✓

   1.0

   b. Where does SES perform substitution and permutation.

   - substitution : S-box inside F ✓
   - permutation : swap LH with RH ✓

   1

   c. Explain SES decryption

   - reverce swap
   - XOR with k
   - reverce F ✓

   1.5

   d. SES performs 16 rounds, which algorithm is better SES or DES? why

   DES, becuse in use F in every round that's mean more substitution operation. but in SES F is done one tim. ✗

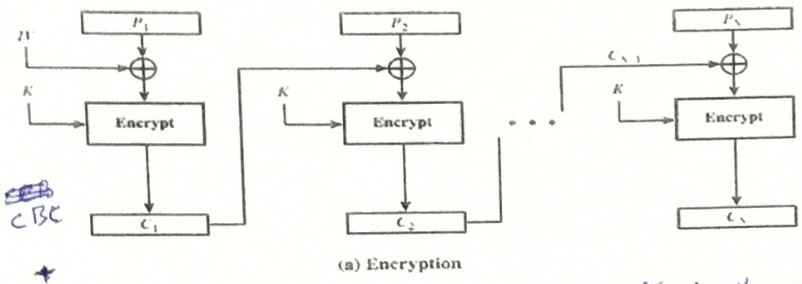
3. Arrange the following ciphers according to the size of their key space (smallest to largest): [ 1 points ]

| | |
|---|---|
| Double DES | caesar ✓ |
| One time pad | Double DES ✓ |
| Caesar | AES ✓ |
| AES | One time Pad ✓ |

1

## Question 4:

1. List one advantage and one limitation of the below mode of operation [ 2 points ]




(a) Encryption

+ one change in any round will effect the rounds after it.
- needs IV, IV mast known by sender and reciver.

2. Encrypting the same information with the same key will result in the same cipher. Propose a solution to the problem that does not involve changing the key. Explain your solution. [ 1 points ]

This problem can solved by usin dinamic Subsetiution operation or dinamic permentation operation, but the problem is the decription function must use same operations.

3. What is the reason of including the following stages in AES [ 2 points ]
   i. Shift Row
      to achive deffusion
   ii. Byte Substituion
      to achive confusion

4. An algorithm designer modified AES Encryption algorithm by swapping the byte substitution and shift row stages. i.e. first perform shift row then byte substitution and claimed that his algorithm is better. Is it? Why? [ 1 points ]

No, changes in stages of AES leads to same cypher text.

5. Which component in AES does not have resemblance in DES. [ 1 point ]

Mix columns.

6. Why the number of rounds is smaller in AES than DES although the block size of AES is larger than DES. [ 1 point ]

change one value effect half of values
because AES can achive (vector) effect after few rounds by mix columns and row shift, but DES needs more round to achive that.

7. Explain what is brute force attack and why it's not the preferred method of attack [ 2 points ]

brute force is trying all posipolitjes to ge key and plain text. it's not preferred because number of posipolitjes is very large and take alot of time.